UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/057,914	01/29/2002	Jens-Peter Redlich	A7995	3714

7590 10/25/2007

SUGHRUE MION, PLLC
2100 Pennsylvania Avenue NW
Washington, DC 20037-3213

EXAMINER	
PATEL, CHIRAG R	
ART UNIT	PAPER NUMBER
2141	

MAIL DATE	DELIVERY MODE
10/25/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/057,914	REDLICH ET AL.	
	Examiner	Art Unit	
	Chirag R. Patel	2141	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 August 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34 and 36-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34 and 36-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Response to Arguments

Applicant's arguments, see Appeal brief - pages 13-19, filed August 27, 2007, with respect to the rejection(s) of claim(s) 1-34, and 36-41 under 35 U.S.C. § 102 and 35 U.S.C. § 103 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Slemmer (US 6,226,677) and Jansen et al. (US 6,243,450). Examiner notes that claim 35 is cancelled by the applicant.

Giniger discloses per Col 2 lines 1-40, "The node device is, for example, an edge device located at a customer premises, or at an Internet POP, a network device located at an intermediate point in the Internet, or can be implemented in software on a computer at the customer premises. The node device includes a data storage containing cryptographic information including information that is private to the node device. The information that is private to the node device can include a private key of a public/private key pair known only to the node device, and can further include a certificate, such as a X.509 format certificate, which includes a public key of the public/private key pair. The node device also includes a tunneling communication service coupled to the network interface and is configured to maintain an encrypted communication tunnel with each of the multiple other node devices using the cryptographic information."

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-22, 24-25, 28-32, 36-37, and 39-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Slemmer (US 6,226,677) in view of Giniger et al. – hereinafter Giniger (US 6,751,729).

As per claim 1, Slemmer discloses a method for performing mutual authentication and authorization of a user's terminal device (U) and an Internet Service Provider (P) in order to establish secure communication between the terminal (U) and a trusted network element (T) to the Internet via an untrusted access station (A) comprising:

establishing an association between a terminal (U) and an untrusted access station (A); (Col 3 line 65 – Col 4 line 18, Figure 1: items 120, 130)

transmitting an ISP authentication packet from terminal (U) to ISP (P) via the untrusted access station (A); (Col 6 line 55 – Col 7 line 52)

sending a user authentication packet from said ISP (P) to said terminal (U) via said untrusted access station (A); (Col 6 line 55 – Col 7 line 52)

wherein a connection is established between the terminal the ISP for trusted network services without providing the terminal with direct access to the internet. (Col 6 line 55- Col 7 line 52)

Slemmer fails to disclose upon authentication of said terminal (U) and said ISP (P), said ISP performs the following: generating a session key;

distributing said session key to said terminal (U) and a trusted network element (T), wherein said session key is used to encrypt traffic between the terminal (U) and the trusted network element (T);

establishing a secure tunnel such that the terminal (U) may communicate with the Internet via said trusted network element (T); wherein said secure tunnel emulates a physical link between the terminal (U) and the trusted network element (T) such that traffic transmitted between the terminal (U) and said Internet via said trusted network element (T) is secure from modification or eavesdropping by said third party access station (A).

Giniger discloses upon authentication of said terminal (U) and said ISP (P), said ISP performs the following: generating a session key; (Col 15 lines 16-22)

distributing said session key to said terminal (U) and a trusted network element (T), wherein said session key is used to encrypt traffic between the terminal (U) and the trusted network element (T); (Col 15 lines 16-22)

establishing a secure tunnel such that the terminal (U) may communicate with the Internet via said trusted network element (T); wherein said secure tunnel emulates a physical link between the terminal (U) and the trusted network element (T) (Col 11 lines 55-58)

such that traffic transmitted between the terminal (U) and said Internet via said trusted network element (T) is secure from modification or eavesdropping by said third party access station (A). (Col 6 lines 14-22, Col 12 lines 14-22)

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to disclose generating a session key; distributing said session key to said terminal (U) and a trusted network element (T), wherein said session key is used to encrypt traffic between the terminal (U) and the trusted network element (T); such that traffic transmitted between the terminal (U) and said Internet via said trusted network element (T) is secure from modification or eavesdropping by said third party access station (A) in the disclosure of Slemmer. The motivation for doing do would have been to provide comprehensive security to guarantee the safe transmission of mission critical data over public networks. (Col 6 lines 14-22).

As per claim 2, Slemmer/ Giniger disclose the method of claim 1. Slemmer discloses the method for performing mutual authentication and authorization of a terminal (U) and an Internet Service Provider (P) in order to establish a secure tunnel between the terminal (U) and a trusted network element to the Internet (T) via an untrusted access station (A) of claim 1, wherein the ISP (P) authentication packet contains an authentication challenge (CH_U) from terminal (U) to ISP (P) to authenticate the identity of ISP (P). (Col 6 line 55- Col 7 line 52)

As per claim 3, Slemmer / Giniger disclose the method for for performing mutual authentication and authorization of a terminal (U) and an Intemet Service Provider (P) in order to establish a secure tunnel between the terminal (U) and a trusted network element to the Internet (T) via an untrusted access station (A) of claim 1. Slemmer discloses wherein the user authentication packet contains an authentication challenge (CH_P) from ISP (P) to the terminal (U) to authenticate the identity of user (U). (Col 6 line 55- Col 7 line 52)

As per claim 4, Slemmer discloses a method for providing public access to IP-based networks via an untrusted infrastructure having untrusted access points comprising:

establishing a connection between an IP-device (U) and said untrusted access point (A), (Col 3 line 65 – Col 4 line 18, Figure 1: items 120, 130)

transmitting an ISP authentication request from said IP device (U) to an intemet service provider (P) affiliated with said IP device (U), wherein said authentication request is transmitted through said untrusted access point (A) affiliated with said untrusted third party owned infrastructure; (Col 6 line 55 – Col 7 line 52, Col 8 line 35-48; an embodiment of the control system implemented for a multi-unit property (e.g., a hotel, an apartment or the like)

transmitting a user authentication request from said ISP (P) to said IP

device (U) to determine whether said IP device (U) is a valid user affiliated with said ISP (P), wherein said authentication request is transmitted through said untrusted access point (A) affiliated with said untrusted third party owned infrastructure; (Col 6 line 55 – Col 7 line 52)

wherein a connection is established between the terminal and the ISP for trusted network services without providing the terminal with direct access to the Internet. (Col 6 line 55- Col 7 line 52)

Slemmer fails to disclose when said ISP (P) authentication request and said user authentication requests is affirmative, said ISP (P): generates a key session for encrypting data packets; and distributes said session key to said IP device (U) and a trusted node (T), wherein said session key is used to encrypt data transmitted between said IP device (U) and said trusted node (T); establishing a secure tunnel as said session key is used to encrypt data packets transmitted between said IP device (U) and said trusted node (T), such that said data packets transmitted between said IP device (U) and an Internet via the untrusted access station (A) are protected from modification and manipulation by said untrusted access station (A) in said secure tunnel, wherein an IP address is dynamically allocated to said IP device.

Giniger discloses generates a key session for encrypting data packets; and distributes said session key to said IP device (U) and a trusted node (T), (Col 15 lines 16-22)

wherein said session key is used to encrypt data transmitted between said IP device (U) and said trusted node (T); establishing a secure tunnel as said session key is

used to encrypt data packets transmitted between said IP device (U) and said trusted node (T), (Col 11 lines 55-58)

such that said data packets transmitted between said IP device (U) and an Internet via the untrusted access station (A) are protected from modification and manipulation by said untrusted access station (A) in said secure tunnel, (Col 6 lines 14-22, Col 12 lines 14-22)

wherein an IP address is dynamically allocated to said IP device. (Col 11line 59 – Col 12 line 2)

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to disclose when said ISP (P) authentication request and said user authentication requests is affirmative, said ISP (P): generates a key session for encrypting data packets; and distributes said session key to said IP device (U) and a trusted node (T), wherein said session key is used to encrypt data transmitted between said IP device (U) and said trusted node (T); establishing a secure tunnel as said session key is used to encrypt data packets transmitted between said IP device (U) and said trusted node (T), such that said data packets transmitted between said IP device (U) and an Internet via the untrusted access station (A) are protected from modification and manipulation by said untrusted access station (A) in said secure tunnel, wherein an IP address is dynamically allocated to said IP device in the disclosure of Slemmer. The motivation for doing do would have been to provide comprehensive security to guarantee the safe transmission of mission critical data over public networks. (Col 6 lines 14-22).

As per claim 5, Slemmer discloses a method for providing public access to IP-based networks through a third party owned, untrusted infrastructure having untrusted access stations (A) comprising:

establishing a connection between an IP-device (U) and said access station (A), (Col 3 line 65 – Col 4 line 18, Figure 1: items 120, 130)

sending an ISP authentication request to said internet service provider (P) affiliated with said IP device (U) requesting to validate the authenticity of the ISP (P); sending a user authentication request from said ISP (P) to said IP device (U) to validate whether said IP device (U) has a service agreement with said ISP (P); (Col 6 line 55 – Col 7 line 52

wherein a connection is established between the terminal and the ISP for trusted network services without providing the terminal with direct access to the Internet. (Col 6 line 55 – Col 7 line 52)

Slemmer fails to disclose upon affirmative authentication of said ISP (P) and said IP device (U); establishing a trusted connection between said IP device (U) and a trusted network element (T), wherein a secure tunnel allows the ISP (P) to dynamically obtain control of resource in said untrusted third party owned access station (A) in order to provide the IP device (U) with prescribed for services, wherein an IP address is dynamically allocated to said IP device (U).

Giniger discloses upon affirmative authentication of said ISP (P) and said IP device (U); establishing a trusted connection between said IP device (U) and a trusted network element (T), wherein a secure tunnel allows the ISP (P) to dynamically obtain

control of resource in said untrusted third party owned access station (A) in order to provide the IP device (U) with prescribed for services, (Col 11 lines 55-58, Col 15 lines lines 16-22)

wherein an IP address is dynamically allocated to said IP device (U); (Col 11line 59 – Col 12 line 2)

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to disclose upon affirmative authentication of said ISP (P) and said IP device (U); establishing a trusted connection between said IP device (U) and a trusted network element (T), wherein a secure tunnel allows the ISP (P) to dynamically obtain control of resource in said untrusted third party owned access station (A) in order to provide the IP device (U) with prescribed for services, wherein an IP address is dynamically allocated to said IP device (U) in the disclosure of Slemmer. The motivation for doing do would have been to guarantee the safe transmission of mission critical data over public networks. (Col 6 lines 14-22)

As per claim 6, Slemmer discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over a third party owned untrusted access station (A) comprising:

establishing a connection between the terminal (U) and said access station (A); sending an ISP authentication request to said internet service provider (P) affiliated with said terminal (U); (Col 3 line 65 – Col 4 line 18, Figure 1: items 120, 130)

sending a user authentication request from said ISP (P) to said terminal (U); (Col 6 line 55 – Col 7 line 52)

wherein a connection is established between the terminal and the ISP for trusted network services without providing the terminal with direct access to the Internet. (Col 6 line 55 – Col 7 line 52)

Slemmer fails to disclose upon affirmative authentication of said ISP (P) and said terminal (U): establishing a trusted connection between said IP device (U) and a trusted network element (T), wherein a secure tunnel allows the ISP (P) to dynamically obtain control of resource in said untrusted access station (A) in order to provide the IP device (U) with prescribed for services.

Giniger discloses upon affirmative authentication of said ISP (P) and said terminal (U): establishing a trusted connection between said IP device (U) and a trusted network element (T), wherein a secure tunnel allows the ISP (P) to dynamically obtain control of resource in said untrusted access station (A) in order to provide the IP device (U) with prescribed for services. (Col 11 lines 55-58, Col 15 lines lines 16-22)

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to disclose discloses upon affirmative authentication of said ISP (P) and said terminal (U): establishing a trusted connection between said IP device (U) and a trusted network element (T), wherein a secure tunnel allows the ISP (P) to dynamically obtain control of resource in said untrusted access station (A) in order to provide the IP device (U) with prescribed for services in the disclosure of Giniger. The

motivation for doing do would have been to guarantee the safe transmission of mission critical data over public networks. (Col 6 lines 14-22).

As per claim 7, Slemmer / Giniger disclose a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6. Slemmer discloses wherein the ISP authentication request contains an authentication challenge (CH_U) from terminal (U) to ISP (P) to authenticate the identity of ISP (P). (Col 6 line 55 – Col 7 line 52)

As per claim 8, Slemmer / Giniger disclose a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6. Slemmer discloses wherein the user authentication request contains an authentication challenge (CH_IP) from ISP (P) to the terminal (U) to authenticate the identity of terminal (U) as having subscribed to said ISP (P) for services. (Col 6 line 55 – Col 7 line 52)

As per claims 9-14, and 37, please see the discussion under claim 1 as similar logic applies.

As per claim 15, Slemmer / Giniger disclose a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with

that terminal and the Internet over an untrusted access station (A) of claim 6. Slemmer fails to disclose a time out is distributed to the trusted node (T) and terminal (U) upon the establishment of a secure tunnel. Giniger discloses a time out is distributed to the trusted node (T) and terminal (U) upon the establishment of a secure tunnel. (Col 12 lines 9-13) At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to disclose a time out is distributed to the trusted node (T) and terminal (U) upon the establishment of a secure tunnel in the disclosure of Slemmer. The motivation for doing do would have been to guarantee the safe transmission of mission critical data over public networks. (Col 6 lines 14-22).

As per claim 16, Slemmer / Giniger discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 15. Slemmer fails to disclose wherein the timeout value is set to a predetermined time period, wherein if the secure tunnel is active for a time period equal to the timeout value, the secure tunnel will expire and the resources utilized for the secure tunnel will be releases. Giniger discloses wherein the timeout value is set to a predetermined time period, wherein if the secure tunnel is active for a time period equal to the timeout value, the secure tunnel will expire and the resources utilized for the secure tunnel will be releases (Col 6 lines 23-27, Col 12 lines 9-13, Col 17 lines 28-34)

As per claims 17-22, please see the discussion under claim 1 as similar logic applies.

As per claims 24-25, 28-30, and 40, please see the discussion under claim 4 as similar logic applies.

As per claim 31, Slemmer / Giniger disclose a method of establishing secure communication between a terminal (U), the Intemet Service Provider (P) affiliated with that terminal and the Intemet over an untrusted access station (A) of claim 6, wherein the untrusted access stations (A) is compatible with at least one wireless transmission standard including WLAN (IEEE 802.11), BlueTooth (IEEE 802.15), or HiperLan. (Col 4 line 64 – Col 5 line 14)

As per claim 32, Slemmer / Giniger disclose a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6. Slemmer discloses wherein the terminal (U) is a mobile device. (Col 6 line 58 – Col 7 line 48)

As per claim 36, Slemmer discloses a method of operating an untrusted access station deployed so as to provide a local network with access to a wide area network, the method comprising:

an untrusted access station receiving a request from a terminal to access trusted network services; (Col 3 line 65 – Col 4 line 18, Figure 1: items 120, 130)

without providing the terminal with direct access to the wide area network, establishing a connection between the terminal and an authentication server for trusted network services performing authentication of the terminal with the authentication server for the trusted network services; (Col 6 line 55 – Col 7 line 52)

Slemmer fails to disclose allowing the terminal to establish a secure channel to trusted network services across the wide area network only if the authentication succeeds. Giniger discloses allowing the terminal to establish a secure channel to trusted network services across the wide area network only if the authentication succeeds. (Col 11 lines 55-58, Col 15 lines 16-22) At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to disclose allowing the terminal to establish a secure channel to trusted network services across the wide area network only if the authentication succeeds in the disclosure of Slemmer. The motivation for doing do would have been to provide comprehensive security to guarantee the safe transmission of mission critical data over public networks. (Col 6 lines 14-22).

As per claim 39, Slemmer / Giniger disclose the method of claim 36. Slemmer disclose wherein the networks are Internet Network Protocol networks. (Col 2 lines 25-44)

Claims 23, 26-27, 34, and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Slemmer (US 6,226,677) / Giniger (US 6,751,729) further in view of Jansen et al. – hereinafter Jansen (US 6,243,450)

As per claims 23, 26-27, and 38, Slemmer / Giniger disclose a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6. Slemmer fails to disclose wherein the ISP (P) provides an accounting of time to the untrusted access station (A) for resources utilized by the terminal (U). Jansen discloses wherein the ISP (P) provides an accounting of time to the untrusted access station (A) for resources utilized by the terminal (U). (Col 2 lines 35-42) At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to disclose wherein the ISP (P) provides an accounting of time to the untrusted access station (A) for resources utilized by the terminal (U). Jansen discloses wherein the ISP (P) provides an accounting of time to the untrusted access station (A) for resources utilized by the terminal (U) in the disclosure of Slemmer. The motivation for doing do would have been to provide a pay-per use billing to end-users of public access services available through an Internet-accessible kiosk or terminal. (Col 1 lines 19-25)

As per claim 34, Slemmer / Giniger discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with

that terminal and the Internet over an untrusted access station (A) of claim 6. Slemmer fails to disclose wherein the untrusted access station (A) assigns an local unique identification (LUID) to the terminal (U) in order to facilitate matching the terminal with data packets when the untrusted access station (A) is simultaneously serving multiple terminals (U). Jansen discloses wherein the untrusted access station (A) assigns an local unique identification (LUID) to the terminal (U) in order to facilitate matching the terminal with data packets when the untrusted access station (A) is simultaneously serving multiple terminals (U). (Col 9 lines 21-35) At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to disclose wherein the untrusted access station (A) assigns an local unique identification (LUID) to the terminal (U) in order to facilitate matching the terminal with data packets when the untrusted access station (A) is simultaneously serving multiple terminals (U) in the disclosure of Slemmer. The motivation for doing do would have been to provide a pay-per use billing to end-users of public access services available through an Internet-accessible kiosk or terminal. (Col 1 lines 19-25)

Claims 33 and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Slemmer (US 6,226,677) / Giniger (US 6,751,729) further in view of Bahl (US 6,957,276).

As per claims 33 and 41, Slemmer / Giniger discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P)

affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6. Slemmer fails to disclose wherein the terminal (U) recognizes a compatible access point by broadcasting a dynamic host configuration protocol (DHCP) request and receiving a "magic" DHCP response from the untrusted access station (A). Bahl discloses wherein the terminal (U) recognizes a compatible access point by broadcasting a dynamic host configuration protocol (DHCP) request and receiving a "magic" DHCP response from the untrusted access station (A). (Col 3 lines 8-27) At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to disclose wherein the terminal (U) recognizes a compatible access point by broadcasting a dynamic host configuration protocol (DHCP) request and receiving a "magic" DHCP response from the untrusted access station (A) in the disclosure of Reference A. The motivation for doing do would have been to reclaim a permanent or static IP address from a machine without having to physically go to the machine. (Col 2 line 65 – Col 3 line 7)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chirag R Patel whose telephone number is (571)272-7966. The examiner can normally be reached on Monday to Friday from 7:30AM to 4:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia, can be reached on (571) 272-3880. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pairdirect.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll free).

Chirag Patel
Patent Examiner
AU 2141

C.P. C.P.

JASON CARDONE
SUPERVISORY PATENT EXAMINER